

How Russia is trying to block Tor

Roger Dingledine

August 12 2022

The Tor Project



Outline

(1) Intro to Tor

(2) Intro to Tor and censorship resistance

(3) What Russia did, when, responses

(4) Bigger context in Russia

(5) Better solutions

(6) What's next

Tor Overview

Online anonymity: open source, open network

Community of devs, researchers, users, relay operators

US 501(c)(3) non-profit organization with 25-30 staff

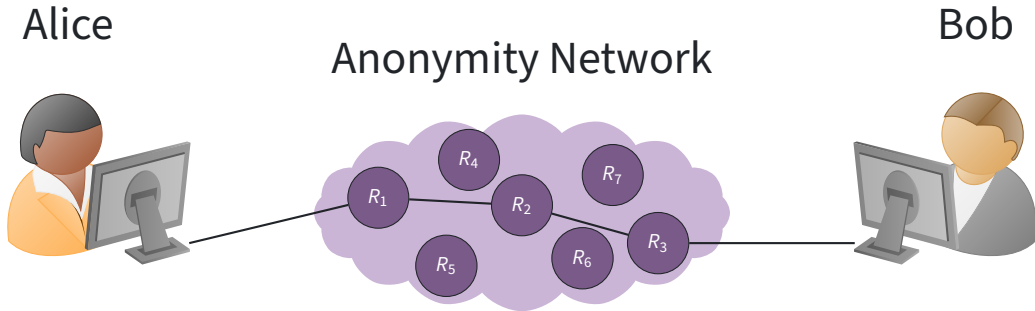
Estimated 2,000,000 to 8,000,000 daily users

Part of larger ecosystems: internet freedom, free software, censorship resistance, anonymity research

History

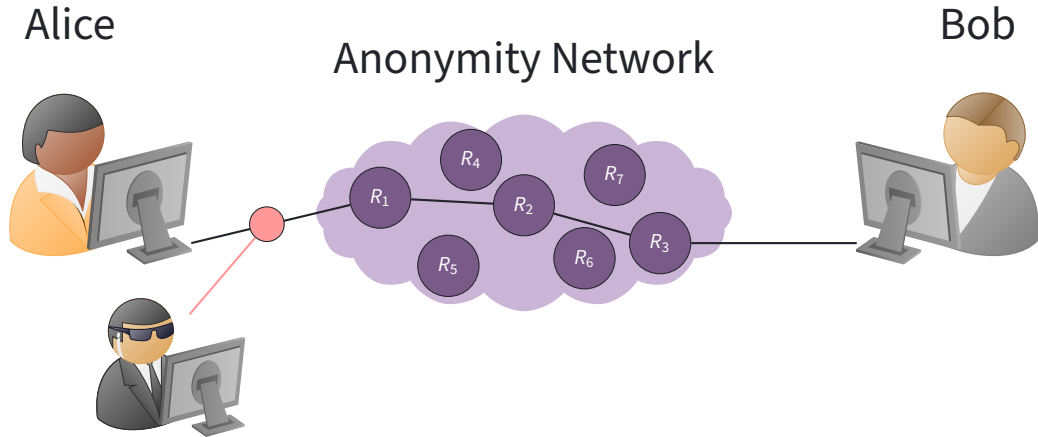
- 2002**– Research with U.S. Naval Research Lab.
- 2004** Sponsorship by Electronic Frontier Foundation.
- 2006** The Tor Project, Inc. became a non-profit.
- 2007** **Expansion to anti-censorship.**
- 2008** Tor Browser development.
- 2010** The Arab spring.
- 2013** The summer of Snowden.
- 2018** **Dedicated anti-censorship team created.**

Threat Model

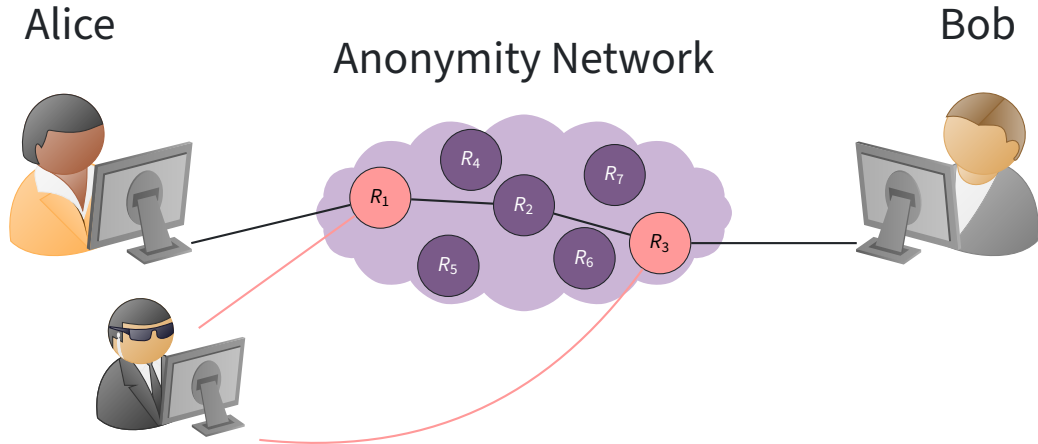


{What can the attacker do?}

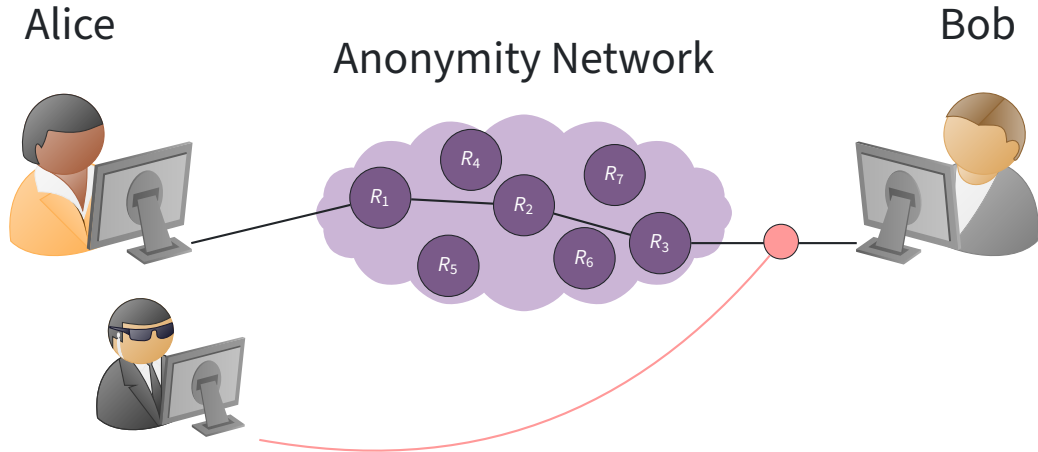
Threat Model



Threat Model



Threat Model

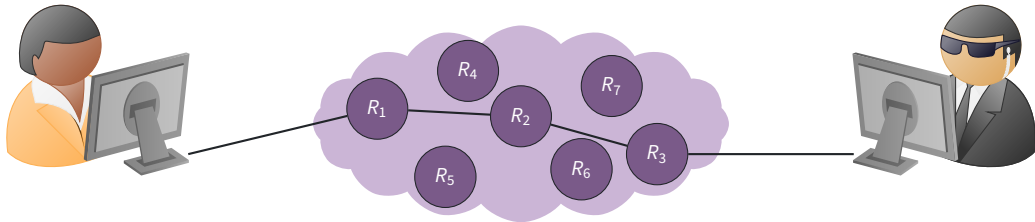


Threat Model

Alice

Anonymity Network

Bob



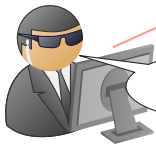
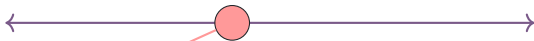
Anonymity isn't Encryption

Alice

Bob



...RG9uJ3QgdXNlIGJhc2U2NCBmb3IgZW5jcnlwdGlvbi4...



Gibberish!

Encryption just protects contents.

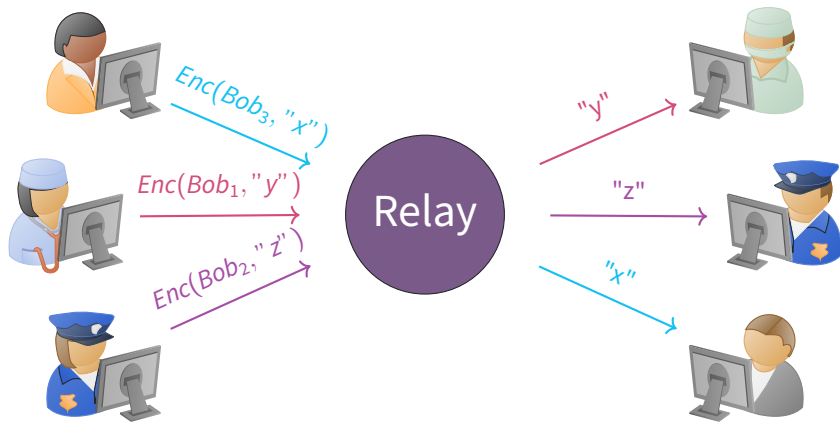
Communications Metadata



"We Kill People Based on Metadata."

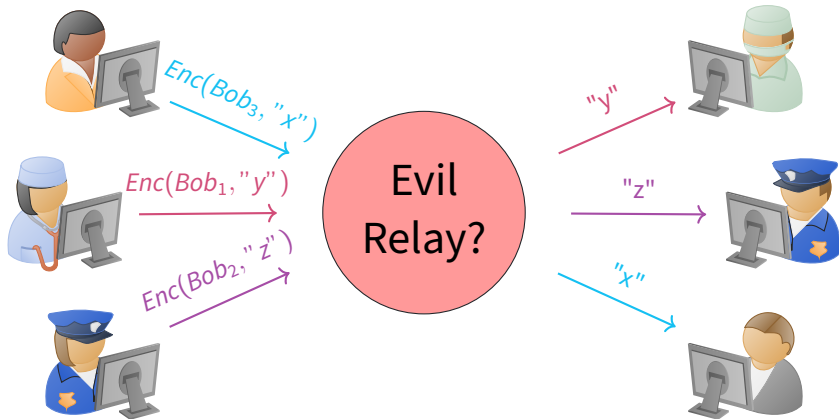
—Michael Hayden, former director, NSA.

A Simple Design

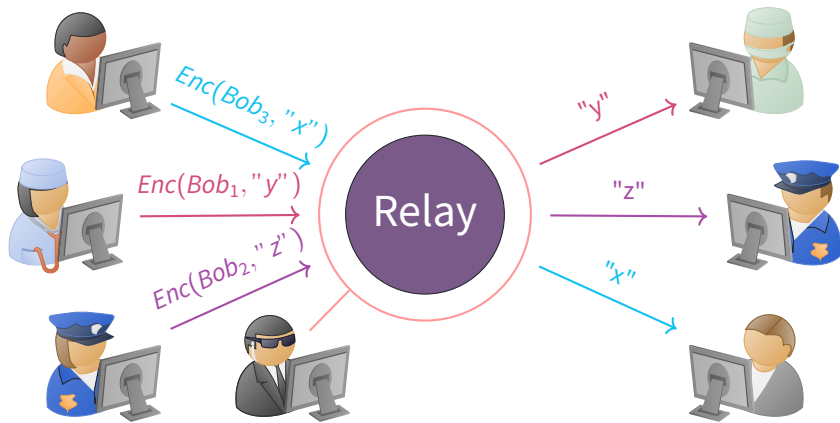


Equivalent to most commercial proxy/VPN providers.

A Simple Design

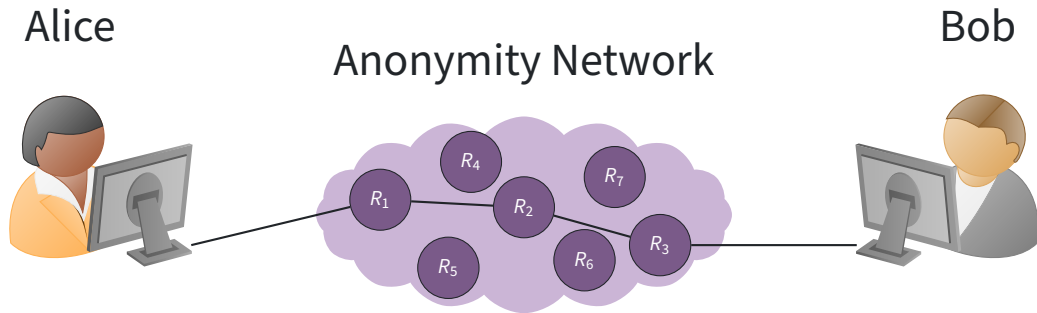


A Simple Design



Timing analysis lets an observer match up connections.

The Tor Design



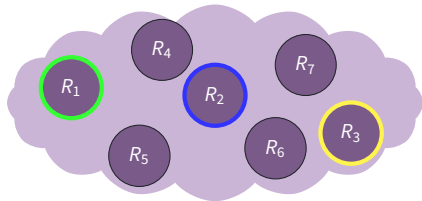
Multiple relays so no single relay can link Alice to Bob.

The Tor Design

Alice



Anonymity Network



Bob



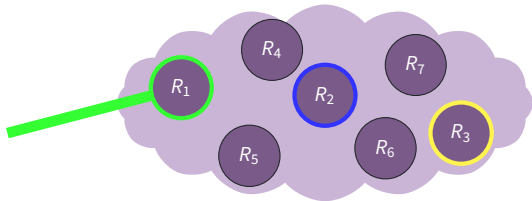
Alice picks a path through the network: R_1 , R_2 , and R_3 before finally reaching Bob.

The Tor Design

Alice

Anonymity Network

Bob



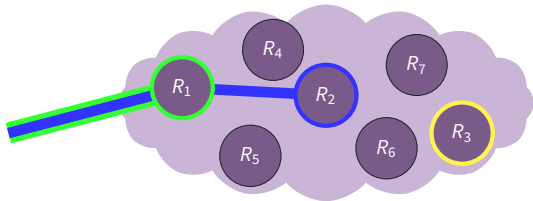
Alice makes a session key with R_1 .

The Tor Design

Alice

Anonymity Network

Bob



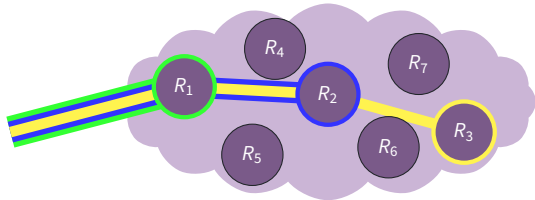
Alice asks R_1 to extend to R_2 .

The Tor Design

Alice

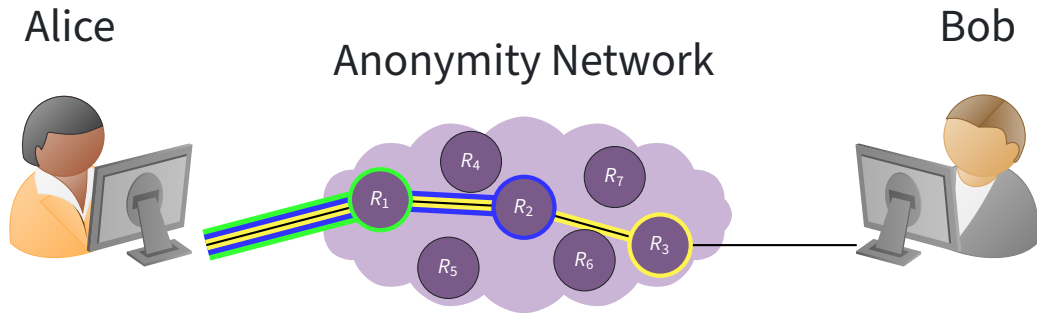
Anonymity Network

Bob



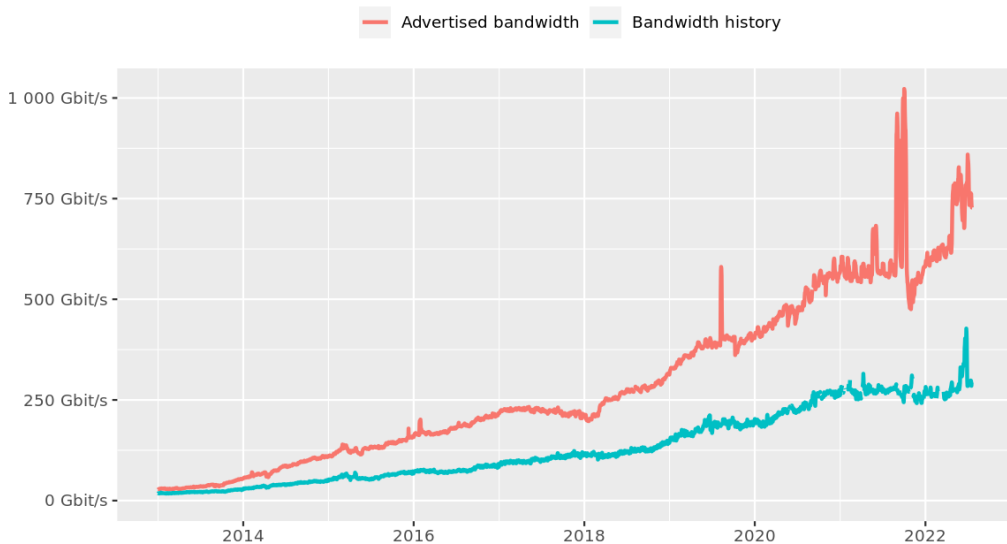
Alice asks R_2 to extend to R_3 .

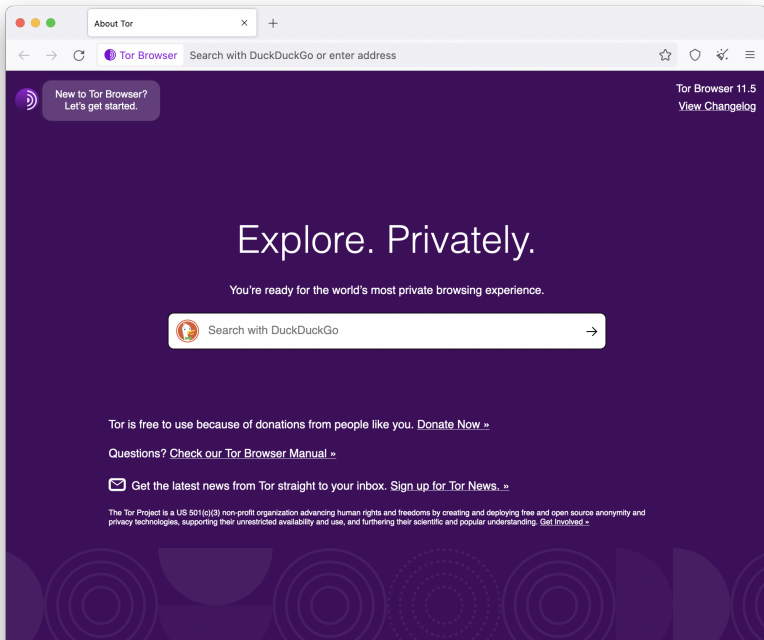
The Tor Design



Alice finally asks R_3 to connect to Bob.

Total relay bandwidth





Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction: privacy is about choice!

Outline

~~(1) Intro to Tor~~

(2) Intro to Tor and censorship resistance

(3) What Russia did, when, responses

(4) Bigger context in Russia

(5) Better solutions

(6) What's next

Bridges, for IP address blocking

The Tor network is made up of 7000 public relays, but the list is public and you can just fetch it and block them by IP address.

So, we have unlisted relays called “bridges” and there is a cat-and-mouse game where users try to get a bridge that the censor didn’t already find.

Pluggable transports, for DPI blocking

Protocol-level arms race too: the Tor protocol looks mostly like TLS, but only if you don't look too carefully.

Rather than perfectly mimicking Firefox+Apache, our “pluggable transports” design aims for modularity:

Tor's three-hop path provides the privacy, and you can plug in different *transports* that transform the first link's traffic into flows that your censor doesn't block.

obfs4 pluggable transport

obfs4 is still the core most successful transport.

It simply adds a new layer of encryption on top, so there are no recognizable headers or formatting at the content layer.

The idea is that automated protocol classifiers won't have any good guesses, so censors are forced to either block all unclassified traffic or allow it all through.

Snowflake pluggable transport

Snowflake makes your traffic look like a WebRTC (zoom, jitsi, skype, signal, etc) call, and those are allowed in many parts of the world.

People can volunteer as Snowflake proxies simply by installing an extension in their browser.

The resulting volume and variety of volunteers gives us more options on how to distribute them to users.

meek pluggable transport

Domain fronting: Makes https request to a shared cloud service (azure, fastly, etc), and tunnels traffic inside it

Outer layer says the SNI (Server Name Indicator) of a popular site, but inner layer has a different Host: header

Have to pay cloud prices for the bandwidth :(, so not great for proxying full traffic flows

Matching bridges to users who need them

Divide obfs4 bridges into distribution buckets, where each bucket relies on a different scarce resource to rate-limit how many bridges the censor can get.

- https (get a few bridges based on your IPv4 /16)
- gmail (get a few bridges based on your username)
- moat (Tor Browser makes a domain-fronted connection, presents a captcha in-browser, and auto-populates your bridge settings).

Matching bridges to users who need them

and Snowflake has a similar “broker” service that matches up Snowflake users to Snowflake volunteers.

Outline

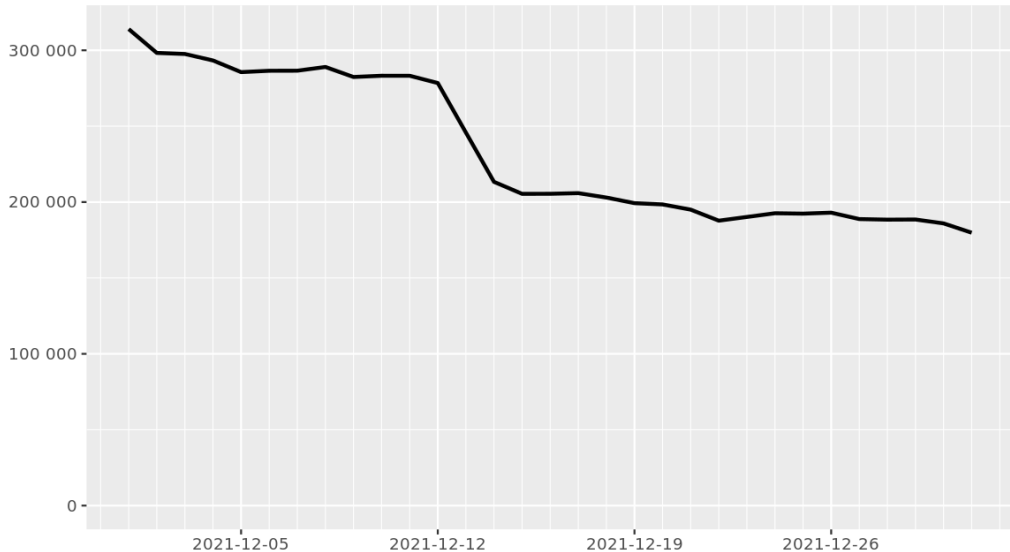
- ~~(1) Intro to Tor~~
- ~~(2) Intro to Tor and censorship resistance~~
- (3) What Russia did, when, responses**
- (4) Bigger context in Russia
- (5) Better solutions
- (6) What's next

Russia, December 2021

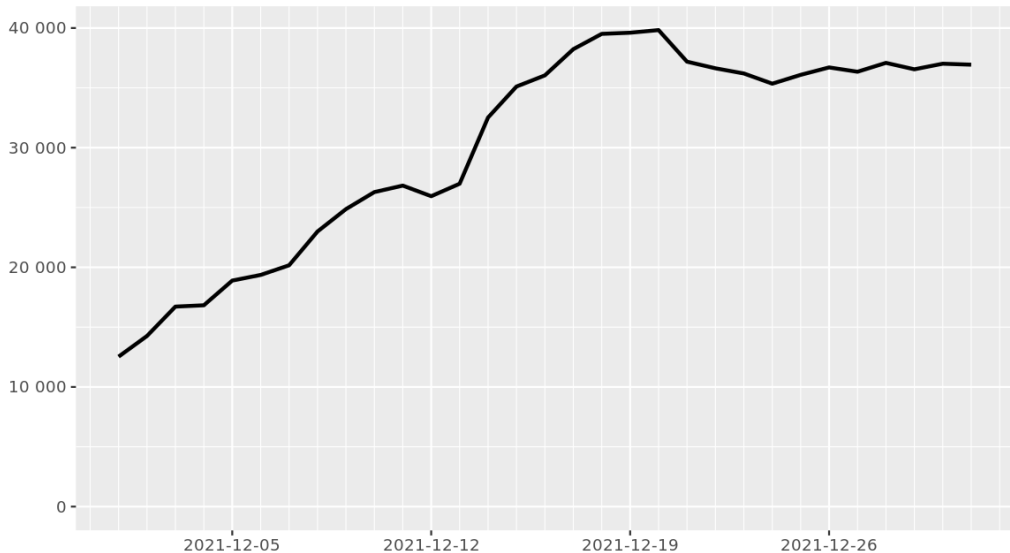
Some ISPs blocked (a) the public Tor relays, (b) meek-azure domain fronting, (c) Tor Browser's default obfs4 bridges, (d) some moat-distributed obfs4 bridges, (e) the Snowflake protocol.

A week later we got an actual legal notice that the Tor website was evil and they were going to censor it. Then they did.

Directly connecting users from Russia



Bridge users from Russia



Only include supported_groups extension for client

[< Prev](#) [Next >](#)

According to <https://www.rfc-editor.org/rfc/rfc8422.html#section-5.1> this extensions are only sent in the ClientHello message of the TLS handshake.

 **cohosh** committed on Dec 8, 2021 Unverified

commit 2f8ef4e48879f1129b3432c9ac04d2f4aad8049e

✓ ↕ 11 ■■■■ flight4handler.go 

...

```
↑... @@ -189,14 +189,9 @@ func flight4Generate(c flightConn, state *State, cache *handshakeCache, cfg *han
189 189     })
190 190     }
191 191     if state.cipherSuite.AuthenticationType() == CipherSuiteAuthenticationTypeCertificate {
192     -     extensions = append(extensions, []extension.Extension{
193     -         &extension.SupportedEllipticCurves{
194     -             EllipticCurves: []elliptic.Curve{elliptic.X25519, elliptic.P256, elliptic.P384},
195     -         },
196     -         &extension.SupportedPointFormats{
197     -             PointFormats: []elliptic.CurvePointFormat{elliptic.CurvePointFormatUncompressed},
198     -         },
```

<



I did some investigations on the meek-azure blocking today. We first thought that they blocked `ajax.aspnetcdn.com` by SNI (which would have been bad enough for collateral damage), but it turns out they blocked the whole IP address `152.199.19.160`, which is what domains like `ajax.aspnetcdn.com`, `clientlogin.cdn.skype.com`, and many many others resolve to in that region of the world.

I set a line in `/etc/hosts` to resolve `ajax.aspnetcdn.com` to a different azure IP address (not really practical as a suggestion for users, but good for doing the test), and meek-azure connected successfully from behind the censorship.

Then [@anadahz](#) suggested I try www.santorini-view.com as a front, since it resolves to a different address, and it works as a front out-of-the-box with meek-azure.

- Conclusion 1, Russia was happy to sign up for significant collateral damage here. Wonder if they thought that through. Maybe they did (see previous run-ins with Russia and domain fronting).
- Conclusion 2, I now believe it makes sense to load up the meek-azure line with a variety of front domains to round-robin among -- and ideally we should pick ones that don't resolve to the same IP address.



No mile...



None



None



2



Russia, mid 2022

Now Russia crawling all three legacy categories of bridgedb obfs4 bridges (moat, https, email)

But still not instantaneous: new bridges last days to weeks

Other obfs4 bridges still work fine

Snowflake and meek continue to work, but are slower

[Sign Up](#)[Log In](#)

Tor blocked in Russia: how to circumvent censorship

[Support](#)[Censorship Circumvention](#)

gus Community Team lead

10 Dec '21

Здравствуйте! Похоже, ваш Интернет-провайдер блокирует Tor. Подробнее об этом см. [OONI reports of Tor blocking in certain ISPs since 2021-12-01 - Russia - NTC](#) 2.4k

Tor Browser включает инструменты обхода блокировок. О том, как использовать мосты Tor, можно прочесть здесь (на русском языке):

- [МОСТЫ | Как стать переводчиком для Tor Project](#) 6.8k
- [TOR ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ | Как стать переводчиком для Tor Project](#) 3.6k

Если у Вас заблокированы вебсайты Tor Project, получить доступ к документации и другим ресурсам проекта можно, воспользовавшись следующими зеркалами:

- [Поддержка Tor](#) 912
- [Руководство пользователя Tor Browser](#) 451
- [Сервис GetTor](#) 700 - только по-английски
- [Запуск собственного моста Tor](#) 1.3k - только по-английски
- [Блог Tor Project](#) 137 - только по-английски
- [Основной вебсайт Tor](#) 794

Dec 2021

1 / 36

Dec 2021

19d ago

177k views!



Tor blocked in Russia: how to circumvent ce...

Support

Censorship Circumvention

Log In



[tor-project] Joydeep's Monthly Status Report for November 2021

Connect to network button after upgrade 2

2021 Fundraising results: thank you! 1

11 more

created



Dec '21

last reply



May 6

43
replies

177k
views

17
users

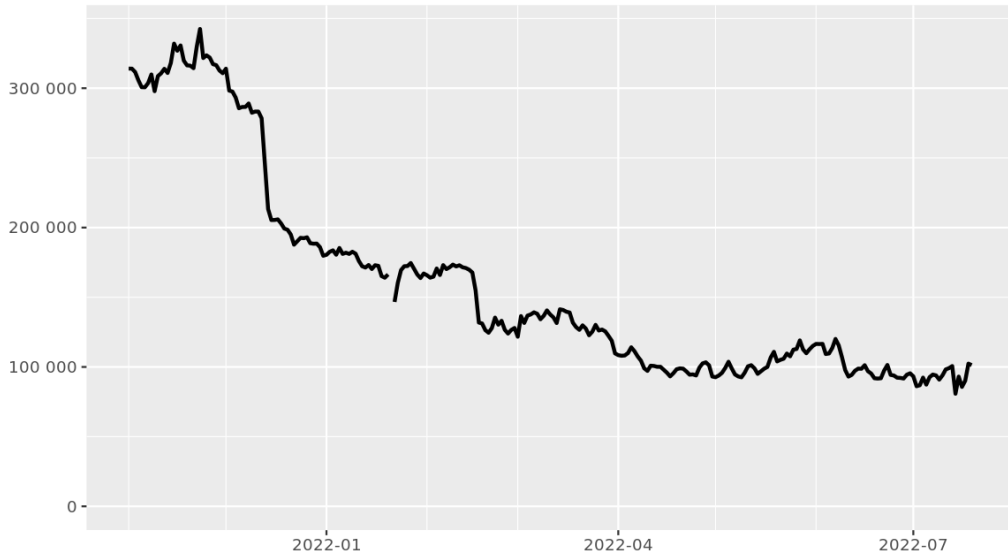
75
likes

46
links



PINNED ON DEC 7, '21

Directly connecting users from Russia



Bridge users from Russia



W



Show an aggressive user count estimate alongside our conservative user count estimate



On our various user graphs on the metrics site, we show a user count that assumes many users are online all day. In countries where many Tor users go online briefly to use Tor and then disappear again (e.g. from modems, internet cafes, etc), our approach means that our user counts in those countries is an underestimate -- by as much as an order of magnitude.

We picked that approach originally because we wanted to be publishing a clearly defensible number, but also because at the time most of our users were on good internet connections (so it wasn't so clearly wrong at first).

I find myself explaining this potential inaccuracy every time I'm showing the graphs to funders. And in the anti-censorship space, I'm often talking to them about exactly the countries where people don't typically leave their Tors running 24/7 on good internet connections.

So my proposal here is to have a "high water mark" line on the user count graphs, to go with our current "low water mark" line. The reality is that the true user count lies somewhere between these two lines, and we don't know where.



Metrics ...



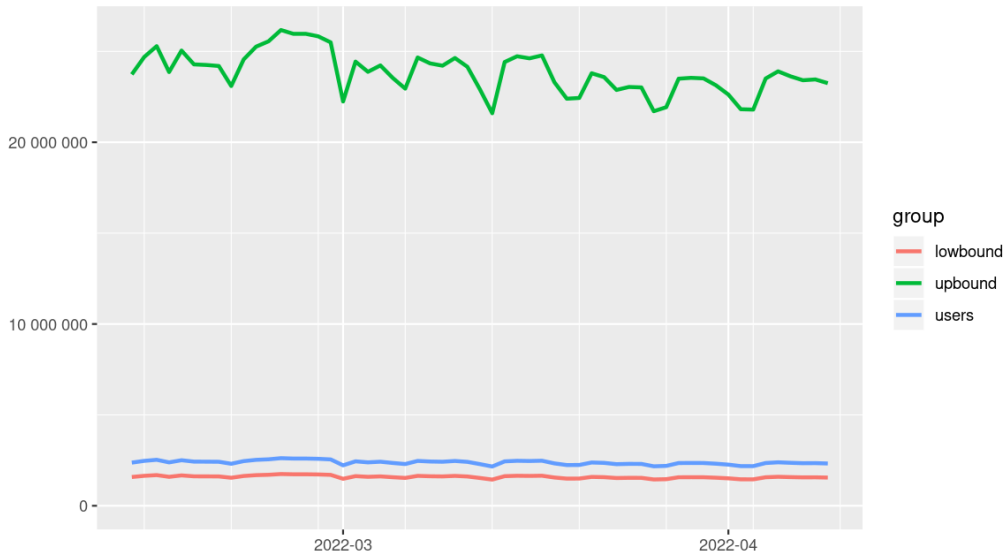
None

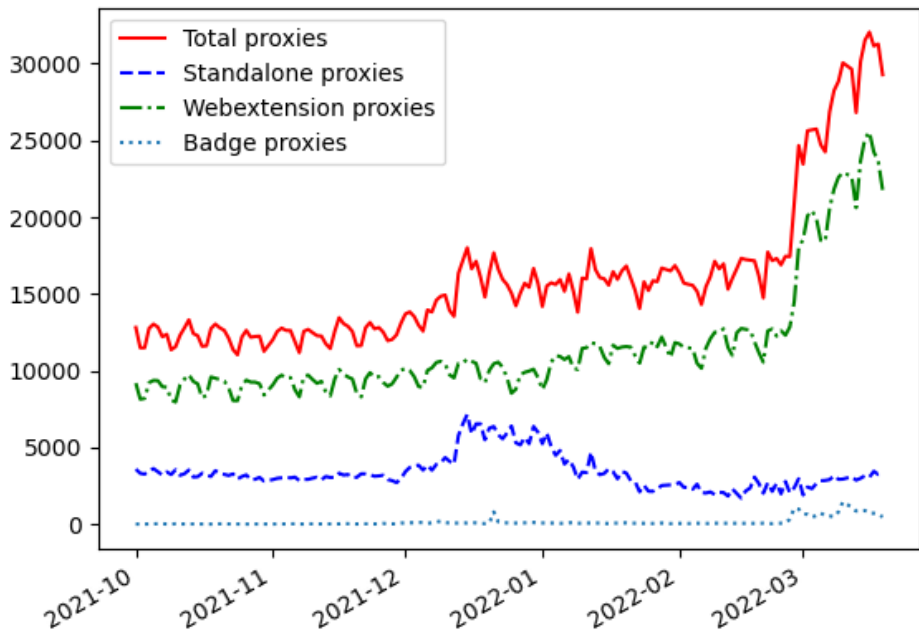


None

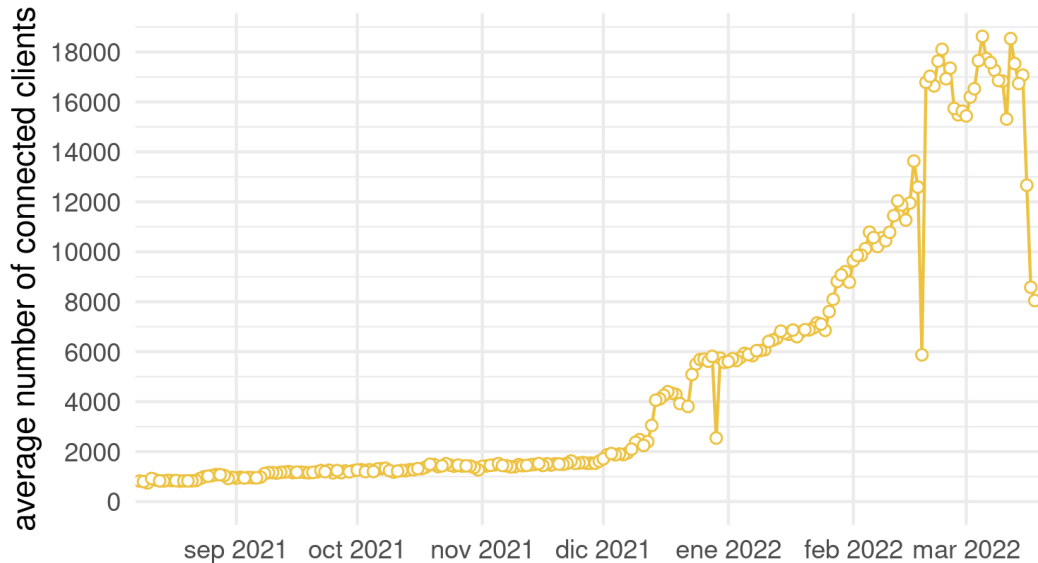


Directly connecting users

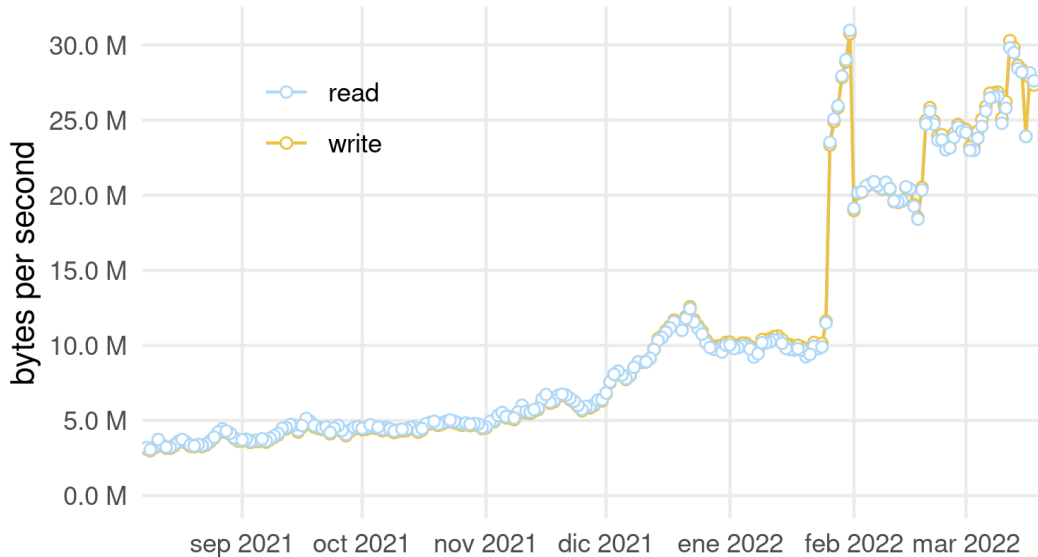




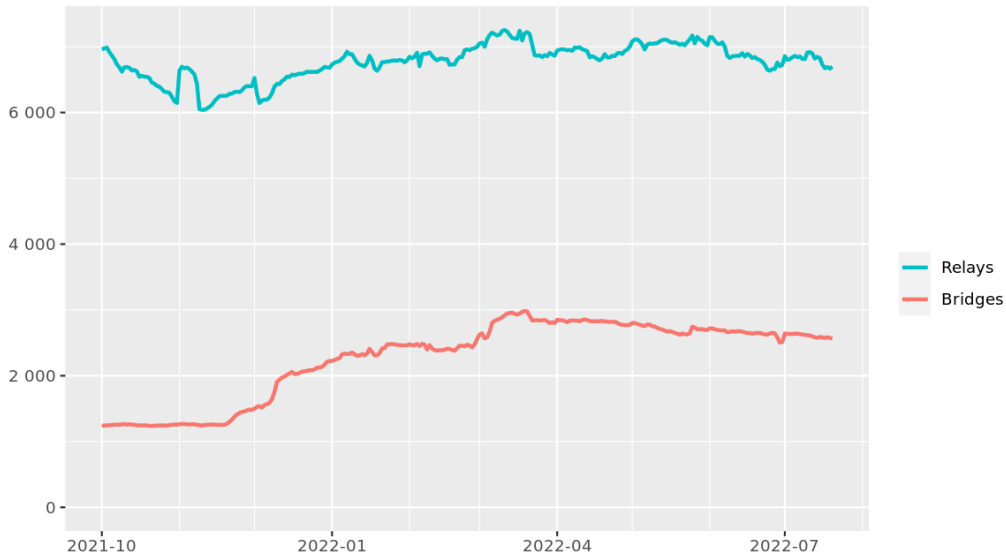
Snowflake clients, combined instances



Snowflake bandwidth history, combined instances



Number of relays



Telegram-based bridge distribution



Tor blocked in Russia: how to circumvent censorship

Support | Censorship Circumvention

Log In

Q

≡



2. запросить мост, используя инструмент Tor Browser - Moat,
3. отправить email по адресу bridges@torproject.org;
4. посетить страницу <https://bridges.torproject.org> 10.8k .
5. или подключиться с помощью Snowflake.

(НОВОСТИ) Как получить мост с помощью Telegram-бота

1. Подключитесь к [@GetBridgesBot](#) 4.5k в Telegram.
2. Наберите `/bridges`
3. Скопируйте всю строку полностью. Ниже рассказано, как вручную добавить мост в Tor Browser.

Как получить мост, используя инструмент Tor Browser - Moat

Российские пользователи могут запрашивать мосты через механизм "запросить мост с [torproject.org](https://bridges.torproject.org) 976 ", встроенный в Tor Browser. Просто выполните следующие три шага:

 Основные

 Начало

Quickstart

Quickstart allows Tor Browser to connect automatically.

Dec 2021

1 / 36

Dec 2021

19d ago

A popular telegram-distributed obfs4 bridge

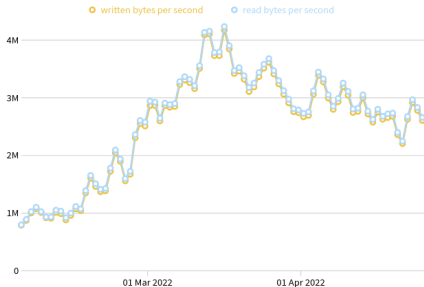
History

1 Month

6 Months

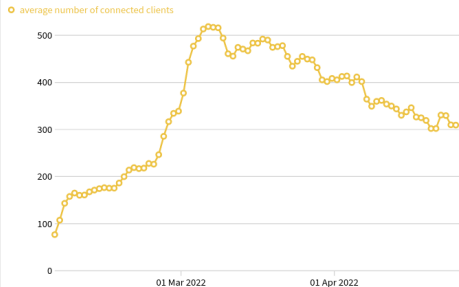
1 Year

5 Years



6 Months graph

Save Graph



6 Months graph

Save Graph



Insider information

<redacted>

Telegram lessons

Other bridge distribution techniques would complement well, e.g. “Use rotating time periods for when we distribute each bridge”

Captcha as a technique is increasingly broken and also increasingly burdensome

Reputation-based bridge distribution designs look well suited for the Russia situation

But still some hard open problems, e.g. sybil resistance

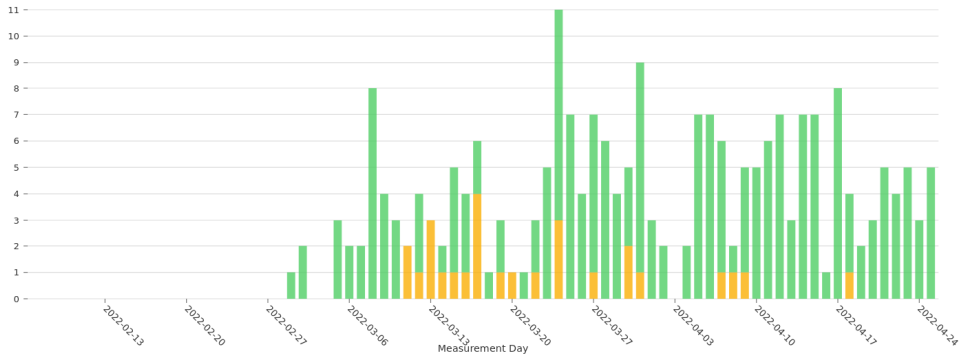
New OONI Snowflake test

- https://explorer.ooni.org/experimental/mat?probe_cc=CN&test_name=torsf&since=2022-02-07&until=2022-03-10&axis_x=measurement_start_day
- <https://github.com/ooni/probe/issues/2004>

China

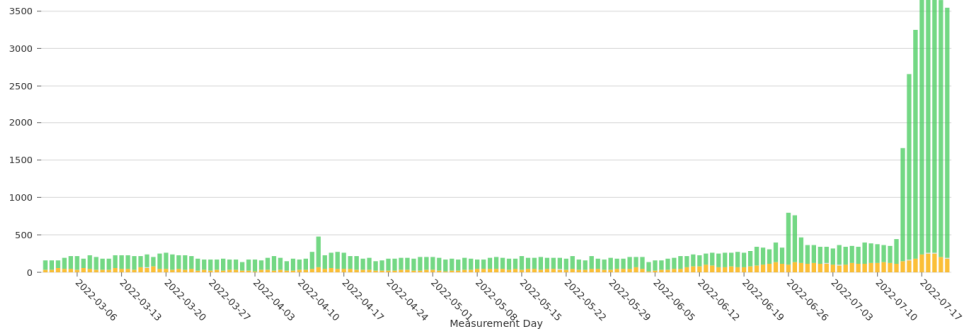
Tor Test

ok_count confirmed_count anomaly_count failure_count



Tor Test

■ ok_count
 ■ confirmed_count
 ■ anomaly_count
 ■ failure_count



...

Sponso...

None

None

Outline

- ~~(1) Intro to Tor~~
- ~~(2) Intro to Tor and censorship resistance~~
- ~~(3) What Russia did, when, responses~~
- (4) Bigger context in Russia**
- (5) Better solutions
- (6) What's next

Challenging the censorship legally

Юридическая команда «Роскомсвободы» теперь [представляет](#) интересы организации **The Tor Project** в России. Наши юристы обжалуют блокировку инструмента на территории страны. [Подробнее об этом читайте на сайте кампании.](#)

«Роскомсвобода» от имени американской общественной организации The Tor Project Inc. обжалует блокировку сайта анонимного браузера в России. <https://t.co/GN8897ITpp>

— Коммерсантъ (@kommersant) [January 24, 2022](#)

Напомним, в декабре 2021 года в России [заблокировали](#) сайт [Tor Project](#), а также публичные прокси-серверы (узлы) и некоторые мосты (непубличные ретрансляторы в сеть Tor). Формальной причиной послужило [Решение саратовского районного суда](#) от 2017 года в соответствии со ст. 15.1 закона «Об информации». Данное решение не касается какого-то определённого контента, в его основании лежит проверка прокуратуры, которая установила, что на сайте проекта Tor есть возможность для «скачивания программы браузера-анонимайзера для последующего посещения сайтов, на которых размещены материалы, включённые в Федеральный список экстремистских материалов».

«Роскомсвобода» считает, что решение суда является незаконным и подлежащим отмене по следующим причинам:

1. решение нарушает конституционное право на свободное предоставление, получение и распространение информации и защиту тайны частной жизни;

Challenging the censorship legally

Google Translate

Russian - detected → English ▼

Translation ▼

⋮

✕

The legal team of Roskomsvoboda now [represents the](#) interests of **The Tor Project** in Russia. Our lawyers will appeal the blocking of the instrument in the country. **Read more about it on the campaign website** .

Roskomsvoboda on behalf of the American public organization The Tor Project Inc. appeals the blocking of the anonymous browser site in Russia. <https://t.co/GN8897ITpp>

— Kommersant (@kommersant) [January 24, 2022](#)

Recall that in December 2021, the [Tor Project](#) website was [blocked](#) in Russia , as well as public proxy servers (nodes) and some bridges (non-public relays to the Tor network). The formal reason was the [decision of the Saratov district court](#) of 2017 in accordance with Art. 15.1 of the Law "On Information". This decision does not apply to any specific content, it is based on a review by the prosecutor's office, which found that the Tor project website has the ability to "download an anonymizing browser program for subsequent visits to sites that host materials included in the Federal List of Extremist Materials ".

Roskomsvoboda believes that the court decision is illegal and subject to cancellation for the following reasons:

1. the decision violates the constitutional right to freely provide, receive and disseminate information and protect privacy;

 Menu

+

▼

🔍

📄 8

🔗 2 ▼

📧 99+

❓ ▼

 ▼

S

Open [Russia] Some ISPs are blocking Tor



Gus 🍕 @gus · 1 month ago

Author Owner 😊 💬 ⋮

Some updates here:

1. [Tor news](#): Ban on Tor's website overturned in Russian court: With the help of digital rights group Roskomsvoboda, we successfully overturned a ban on the Tor Project's website (torproject.org) in Russia! This means that the Russian governmental agency responsible for censorship will have to remove Tor from its block list. We will be returning to court for more hearings and litigation, and this time, Google is included as a third party in the case, **as the Russian authorities are demanding that Tor Browser for Android be removed from the Play Store**. We will keep you updated on new developments as they happen.
<https://roskomsvoboda.org/post/google-v-dele-tor/>

2. Sandvine stopping all sales in Russia:"Since Russia's invasion of Ukraine, Sandvine has pulled back on its Russia work, stopping all sales in the country, a spokesperson said. In addition, the spokesperson said the company's equipment was used in Russia for billing and "quality of service" and not to censor the internet." <https://www.bloomberg.com/news/articles>

⏪



📄 3

🕒 No mil...

📅 None

🕒

⏩

60

Censorship authority dox



[Main page](#)
[About](#)
[Donate](#)
[FAQ](#)
[Contact](#)
[Recent changes](#)

Tools

[What links here](#)
[Related changes](#)
[Special pages](#)
[Printable version](#)
[Permanent link](#)
[Page information](#)

[Page](#) [Discussion](#) [Read](#) [View source](#) [View history](#)

Roskomnadzor

Over 360,000 files from the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (previously the Russian Federal Surveillance Service for Compliance with the Legislation in Mass Media and Cultural Heritage Protection), often abbreviated and referred to as Роскомнадзор or Roskomnadzor. Roskomnadzor is the Russian agency responsible for monitoring, controlling and censoring Russian mass media as well as compliance with personal data processing requirements and coordinating activities involving radio frequencies.

Roskomnadzor's activities are always a matter of public interest to the people of Russia and to

RELEASE

Roskomnadzor / Роскомнадзор

Over 360,000 files from Roskomnadzor, the Russian agency responsible for monitoring, controlling and censoring Russian mass media.

Более 360,000 файлов Роскомнадзора, Российского агентства, отвечающего за наблюдение, контроль и цензуру СМИ России.

DATASET DETAILS

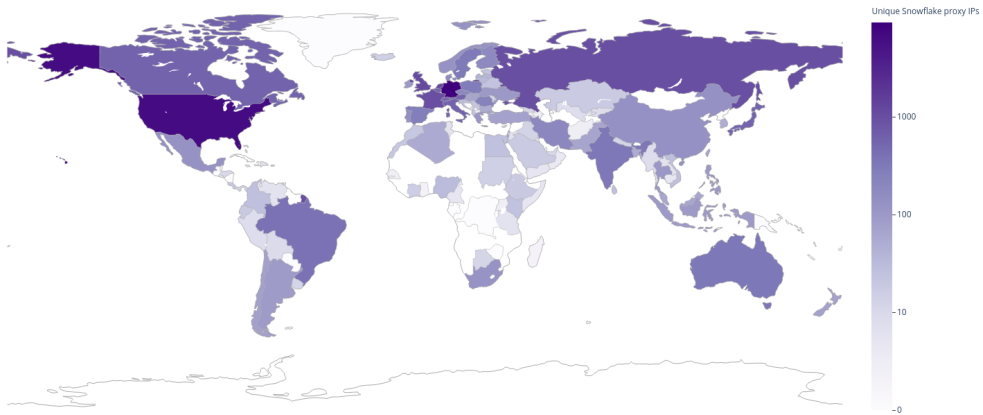
COUNTRIES Russia

TYPE Hack

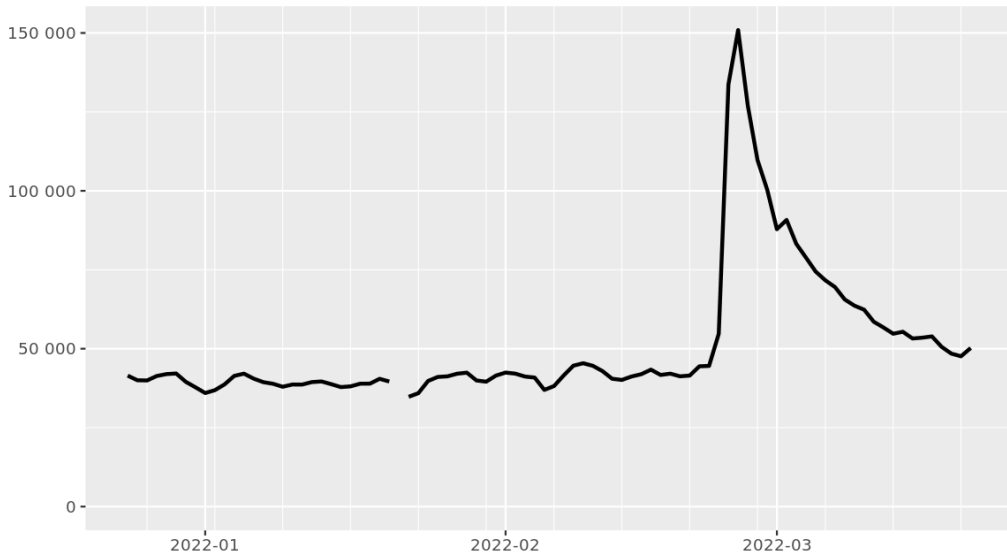
Other surprises

- rt.com censored from many Tor exits, because Europe (i.e. France, part of Germany, maybe more now?) pledged to censor it.
- Actually, many Tor exits can't reach sites in Russia now, because the blocking is bidirectional?
- New groups of Russian and Ukrainian exit relays, “hmm”

Distribution of Snowflake proxies July 20 2022



Directly connecting users from Ukraine



Down the road of the arms race (1/2)

Consider *user impact* from the censorship arms race.

Yes, we have steps to counter each step the censor takes. But as we move down that path, users have a higher burden to achieve a working connection.

Down the road of the arms race (2/2)

We see this user drop-off effect already, where the number of Tor users who switched over to bridges is impressive, but it's definitely not all of them.

We need to find ways to reduce that burden, and/or slow down the arms race, else the censor wins because the average user won't care enough to bother.

Outline

- ~~(1) Intro to Tor~~
- ~~(2) Intro to Tor and censorship resistance~~
- ~~(3) What Russia did, when, responses~~
- ~~(4) Bigger context in Russia~~
- (5) Better solutions**
- (6) What's next

Building block 1

#1: a DPI-resistant point-to-point channel.

That's obfs4, but it can also be v2ray's vmess or any similar project.

Building block 2

#2: a Sybil-resistant sign-up mechanism.

moat/https/gmail buckets are a good start, but Telegram distributor (with twist) is a better start.

Need to identify resources where (a) individual users probably have a few but it's tough for the censor to have many, and (b) it's easy to verify in an automated way.

Think “Facebook accounts” or “friends on Twitter”

Building block 3

#3: a way to establish ground-truth about a suspected-blocked bridge.

bridgestrap “obfs4 reachability” tool

Index of /archive/bridgestrap

	Name	Last modified	Size	Description
	Parent Directory		-	
	bridgestrap-2021-08.tar.xz	2021-09-07 14:53	26K	
	bridgestrap-2021-09.tar.xz	2021-10-07 13:55	108	
	bridgestrap-2021-10.tar.xz	2021-11-07 21:38	108	
	bridgestrap-2021-11.tar.xz	2021-12-08 21:01	69K	
	bridgestrap-2021-12.tar.xz	2022-01-08 03:09	113K	
	bridgestrap-2022-01.tar.xz	2022-02-10 16:18	127K	
	bridgestrap-2022-02.tar.xz	2022-03-08 17:10	143K	
	bridgestrap-2022-03.tar.xz	2022-03-24 09:16	159K	

Apache Server at collector.torproject.org Port 443

```
@type bridgestrap-stats 1.0
bridgestrap-stats-end 2022-03-23 08:29:07 (86400 s)
bridgestrap-cached-requests 137710
bridgestrap-test true 005FD4D7DECBB250055B861579E6FDC79AD17BEE
bridgestrap-test true 00782946F4C54CE1D028F21E541EF8440ECA0EE
bridgestrap-test true 00A4295A8477453D6AFE1CA4C2F19E3708E63FC4
bridgestrap-test true 00A4295A8477453D6AFE1CA4C2F19E3708E63FC4
bridgestrap-test true 00E1AE6CB75E47E363E6AEF9F67A49C0E854FDE7
bridgestrap-test true 00E6F1D633D4E29DB31F43D1E6E3E928E5C1810D
bridgestrap-test true 0110A6CF41A07637808FFF79C0783FF37462B525
bridgestrap-test true 01292375AE04F41E7453D8E85DF446C22A8D7101
bridgestrap-test true 01341C9B4BC01B3A11E80A645A0BDE45DB02F04B
bridgestrap-test false 01341C9B4BC01B3A11E80A645A0BDE45DB02F04B
bridgestrap-test false 01436EF5B118FD95004A75F4616A6094D4AA4748
bridgestrap-test true 0145C4524211A250519864627E4AE31EECCCD39F
bridgestrap-test false 01520C1BB2C46BF0F54969B71217BE04C1F8EB58
bridgestrap-test true 01559EB6040D14F40AAC8CEE0663D1C3CFD449A9
bridgestrap-test true 0177D63957BD0D80319DE36BB09AF4E27CA75ED6
bridgestrap-test true 018CD1182D56FA354AEBC08D9AF2B9DB40194E76
bridgestrap-test true 01B525EE79B66B9CADC030D19B4C3D28DE0F7C18
bridgestrap-test true 01DF57F4B91E610C000436FCD55FA2B2B47BBF39
bridgestrap-test true 01DF57F4B91E610C000436FCD55FA2B2B47BBF39
bridgestrap-test true 01E85E61DB8BFC5606591BB867A76CCDCA1D395D
bridgestrap-test false 01EE817ACE40C0CE10AE9C0C23A72AA6C863F139
```

Centralized probe log collection

- <https://gitlab.torproject.org/tpo/anti-censorship/team/-/issues/54>
- First vantage points in China, Turkey, Russia, Ukraine
- Emphasis on more frequent testing because partial (slow) bootstrap results are more common than we first expected

Building block 4

#4: a large pool of diverse bridge addresses.

There are two pieces to this: one is the group of thousands of volunteers who run their own bridges.

The second is an automated framework for easily spinning up and down bridge images on popular cloud providers.

Dynamic bridges, easy to rotate

[Home](#) » [Services](#) » [Relay Search](#) » Search for sr2

Relay Search

sr2

sr2

Show 10 entries

Nickname [†]	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
● Sr2SilverWipe	17.86 MiB/s	49d 3h		IPv4	IPv6	↑↓	⚡		0	Bridge
● Sr2SilverUmbrella	15.1 MiB/s	49d 3h		IPv4	IPv6	↑↓	⚡		0	Bridge
● Sr2SilverSupply	14.21 MiB/s	49d 3h		IPv4	IPv6	↑↓	⚡		0	Bridge
● Sr2SilverScreener	12.74 MiB/s	9d 23h		IPv4	IPv6	↑↓	⚡		0	Bridge
● Sr2IronDaffodil	10.72 MiB/s	66d 20m		IPv4	-	↑↓			0	Bridge
● Sr2IronDinosaur	10.66 MiB/s	66d 20m		IPv4	-	↑↓			0	Bridge
● Sr2IronTelegraphy	10.53 MiB/s	49d 3h		IPv4	-	↑↓			0	Bridge
● Sr2IronBaguette	10.34 MiB/s	42d 5h		IPv4	-	↑↓			0	Bridge
● Sr2IronPound	9.14 MiB/s	42d 5h		IPv4	-	↑↓			0	Bridge
● Sr2PlasticDrone	9.03 MiB/s	1d 16h		IPv4	IPv6	↑↓	⚡		0	Bridge
Total	384.6 MiB/s									

Showing 1 to 10 of 66 entries

Previous 1 2 3 4 5 6 7 Next



Building block 5

#5: a robust signaling channel.

Need some bidirectional channel that will reliably work, i.e. that censors won't want to block even when they know the details of how it works.

It's fine if it's low-bandwidth and not-great-latency.

Domain fronting through Fastly; proxy through Google AMP cache; tunnel through DoH or email.

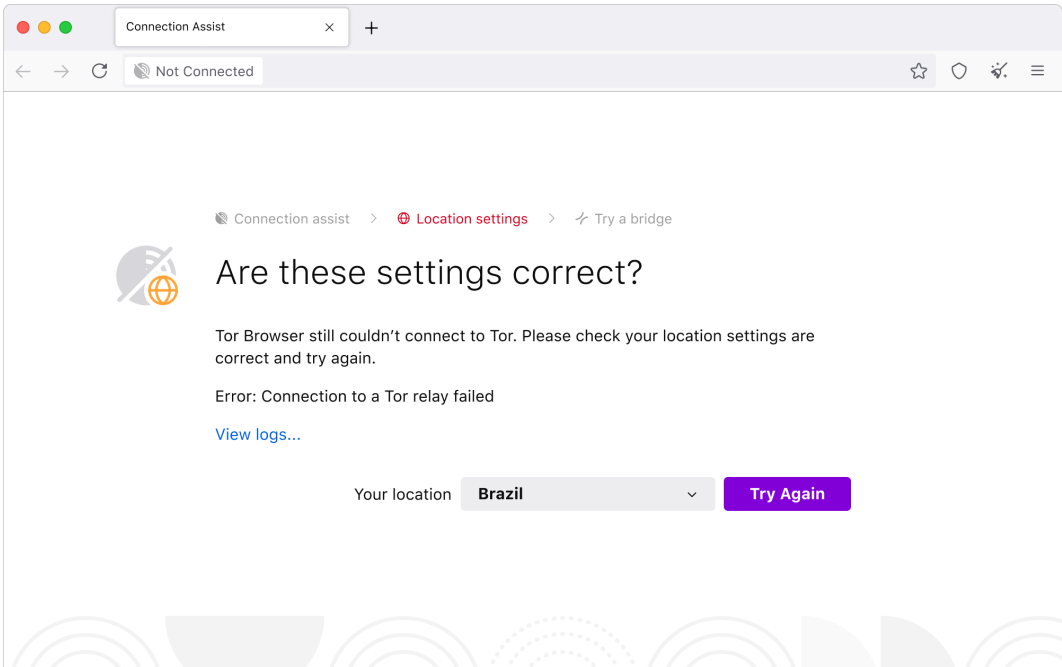
Milestone 1: Tor Browser automation

Tor Browser uses the signaling channel to learn the recommendations for your country.

It fetches a json file with an ordered list of which pluggable transports and which bridge distribution strategies are expected to work best in each country.

Then Tor Browser walks the user through trying them.

```
{
  "by": {
    "settings": [
      {"bridges": {"type": "obfs4", "source": "builtin"}},
      {"bridges": {"type": "vanilla", "source": "bridgedb"}},
      {"bridges": {"type": "obfs4", "source": "bridgedb"}},
      {"bridges": {"type": "snowflake", "source": "builtin"}}
    ]
  },
  "cn": {
    "settings": [
      {"bridges": {"type": "snowflake", "source": "builtin"}}
    ]
  },
  "tm": {
    "settings": [
      {"bridges": {"type": "obfs4", "source": "bridgedb"}},
      {"bridges": {"type": "snowflake", "source": "builtin"}}
    ]
  },
  "ru": {
    "settings": [
      {"bridges": {"type": "snowflake", "source": "builtin"}},
      {"bridges": {"type": "obfs4", "source": "bridgedb"}}
    ]
  }
}
```



[Home](#)[Search](#)[Privacy & Security](#)[Connection](#)[Extensions & Themes](#)[Tor Browser Support](#)

Connection

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world. [Learn more](#)

**Internet:** Online[Test Again](#)**Tor Network:** Potentially Blocked

Quickstart

Quickstart connects Tor Browser to the Tor Network automatically when launched, based on your last used connection settings. [Learn more](#)

☐ Always connect automatically

Bridges

Bridges help you access the Tor Network in places where Tor is blocked. Depending on where you are, one bridge may work better than another. [Learn more](#)

Your location

Automatic

[Choose a Bridge For Me...](#)

Add a New Bridge

Choose from one of Tor Browser's built-in bridges

[Select a Built-In Bridge...](#)

Request a bridge from torproject.org

[Request a Bridge...](#)

Enter a bridge address you already know

[Add a Bridge Manually...](#)

Advanced

Configure how Tor Browser connects to the internet

[Settings...](#)

View the Tor logs

[View Logs...](#)

Milestone 2: Bridge “subscription” model

Short-lived bridges are a reliability problem, separate from censorship.

With Tor Browser automation, next step use the signaling channel to ask for a replacement bridge.

You use the old bridge as the credential to prove that you deserve a new one—skipping the proof-of-resource step so it can all happen in the background.

Dynamic cloud bridges

The subscription model makes the dynamic cloud bridge approach much more powerful: if a bridge gets blocked anywhere, you can spin it down and spin up a new one somewhere else, and users will be able to follow their bridge.

But there is a tradeoff: censors can block a bridge they know and then follow it and block its replacement, etc.

Milestone 3: Trust-based distribution (1/2)

(designs like Salmon, rBridge, Hyphae, Lox)

With Tor Browser doing background connections to maintain your bridges, now rather than just replacing bridges when they die, instead track whether the bridges you gave somebody got blocked.

Get rid of users whose bridges tend to get blocked, and reward users whose bridges last a long time.

Milestone 3: Trust-based distribution (2/2)

Need to pick the right parameters so good users get enough bridges yet bad people can't find too many.

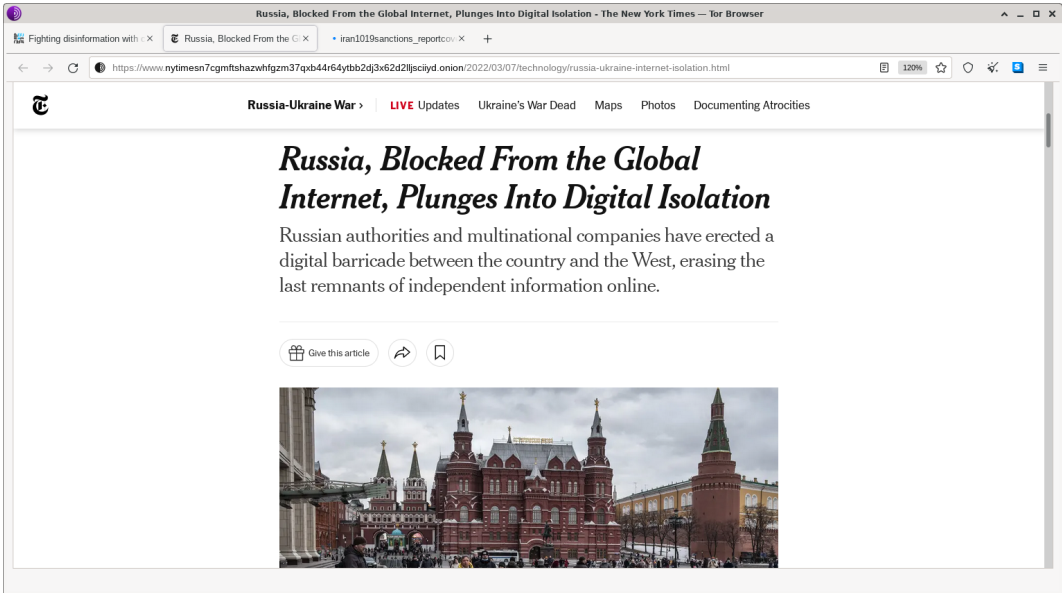
Salmon lets trusted users invite friends to higher trust levels; if a user misbehaves blame their sponsor too.

But...privacy-preserving social graph management?

This is where the arms race needs to go: focus on *exploiting asymmetries* against well-funded censors.

Outline

- ~~(1) Intro to Tor~~
- ~~(2) Intro to Tor and censorship resistance~~
- ~~(3) What Russia did, when, responses~~
- ~~(4) Bigger context in Russia~~
- ~~(5) Better solutions~~
- (6) What's next**



First, a rant about sanctions

Especially about hurting internet connectivity for people in Russia as a way to punish their government.

Compare to the effects of Trump's "maximum pressure" sanctions against Iran.

We will see the same outcome in Russia.



[Home](#) > [Press](#) > [Press releases](#)

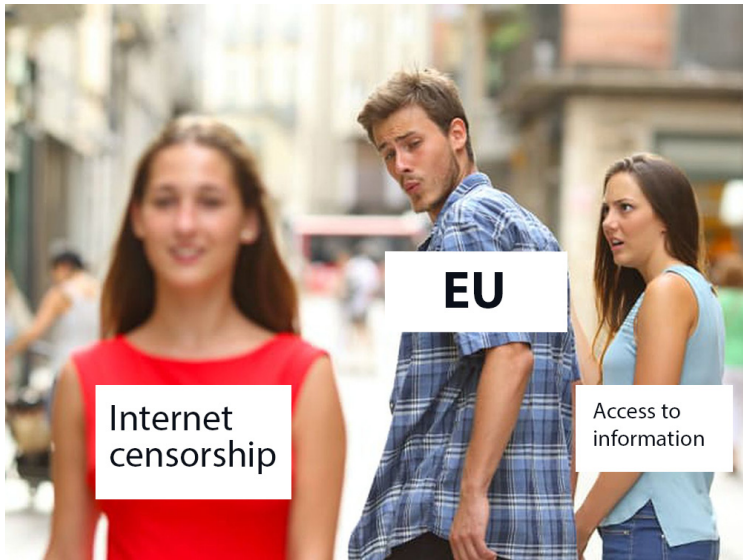
Council of the EU Press release 2 March 2022 12:40

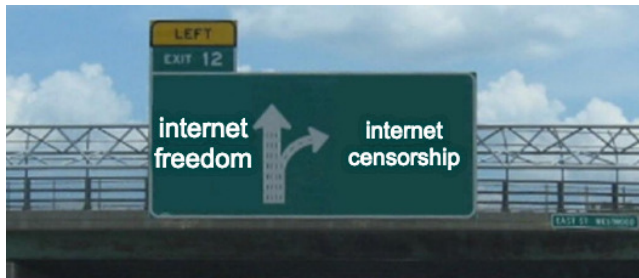
EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU

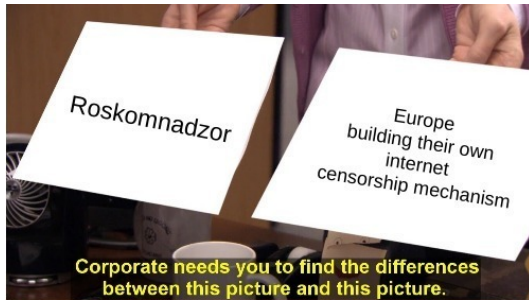
The Council today introduced further restrictive measures in response to Russia's unprovoked and unjustified military aggression against Ukraine. By virtue of these measures, the **EU will urgently suspend the broadcasting activities of Sputnik' and RT/Russia Today** (RT English, RT UK, RT Germany, RT France, and RT Spanish) in the EU, or directed at the EU, until the aggression to Ukraine is put to an end, and until the Russian Federation and its associated outlets cease to conduct disinformation and information manipulation actions against the EU and its member states.



Systematic information manipulation and disinformation by the Kremlin is applied as an operational tool in its assault on Ukraine. It is also a significant and direct threat to the Union's public order and security. Today, we are taking an important step against Putin's manipulation operation and turning off the tap for Russian state-controlled media in the EU. We have already earlier put sanctions on leadership of RT, including the editor-in-chief Simonyan, and it is only logical to also target the activities the organisations have







WTF Europe?? Why u like
censoring so much??

Internet censorship: early warning system

Notice that our Russia Tor blocking story started at the beginning of December 2021.

From the rest of the world's perspective, the Russia story started in February 2022.

So (a) yeah they knew this was coming, and (b) internet censorship often serves as an early warning system for upcoming political events.

GFW blocking by too much entropy

China is experimenting with blocking based on flow-level entropy: if the first k characters in the flow are too random, they kill it.

Only doing it to flows destined for certain cheapo providers like Hetzner, OVH, Digital Ocean, Alibaba.

Maybe they can't tolerate the collateral damage from doing it more widely? Or, maybe they can?

We're going to need better transports.



Calls to action

Please run bridges!

Please run Snowflakes!

Please run relays!

Please participate in the anti-censorship research community!

Ongoing Q&A at the Tor booth in the vendor area!